Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

CITY OF BEND

Information Technology Acceptable Use

Policy No. IT-0001

City Manager Administrative Policy

Bend Code Chapter 1.30.005 provides for 'City Manager Authority to Adopt Administrative Regulations, Policies and Guidelines.' All regulations, policies and guidelines adopted by the City Manager shall be consistent with the City of Bend Charter, the Bend Code, and council ordinances.

The following policy conforms to the above stated standards.

Authorized by City Manager:

DocuSigned by:
Eric King
409FF33EB4E64D3...

Eric King, City Manager

Dated: 4/30/2025

Reviewed by Legal Counsel:

Signed by:
Ian M. Leitheiser
392FD2178C27458...

Ian Leitheiser, City Attorney

Dated: 4/30/2025

Policy No. IT-0001
Adopted: 04/30/2025
Owner: Information Technology Department

Revised:
Revision No.

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

I. Purpose

The purpose of this Policy is to outline the acceptable use of City Systems at the City of Bend. Inappropriate and unacceptable use exposes the City of Bend to risks including system attacks, compromise of City Systems and services, and legal, financial, compliance, and other risks and issues.

II. Policy Statement

It is the City of Bend's policy to ensure the secure and proper use of all City Systems. This Policy outlines the acceptable use of City Systems, which include each and every information technology and communication resource, platform, tool, network, and application, both hardware and software, provided, maintained, and/or made available by the City of Bend. Becoming an authorized user of City Systems requires authorization from the City of Bend Information Technology (IT) Department.

III. Scope

All users of City Systems.

IV. Definitions

Spam: Unauthorized and/or unsolicited electronic mass mailings.

City Systems or "Systems": An integrated set of components designed for collecting, storing, and processing data.

Artificial Intelligence (AI): AI refers to the development of computer systems that can perform tasks typically requiring human intelligence. These systems learn from experience, adapt to new information, and can perform tasks like natural language understanding, problem-solving, and decision-making.

Virus: A virus is a type of malicious software that attaches itself to legitimate programs or files. When executed, it replicates and spreads to other files, potentially causing damage to data, applications, or the system.

Worms: Worms are self-replicating programs that spread across networks without user intervention. Unlike viruses, they do not need a host file to propagate. Worms can consume network resources and cause disruptions.

Trojan Horses: Trojans appear harmless but contain hidden malicious code. Users unknowingly execute them, leading to unauthorized access, data theft, or system compromise. Unlike viruses and worms, Trojans do not self-replicate.

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

Malware: Malware (short for "malicious software") encompasses various harmful programs, including viruses, worms, Trojans, spyware, and ransomware. Its purpose is to disrupt, damage, or gain unauthorized access.

Security Breach: A security breach occurs when unauthorized individuals gain access to sensitive information, systems, or networks. Breaches can result from vulnerabilities, weak passwords, or misconfigurations.

Network Sniffing: Network sniffing involves capturing and analyzing network traffic to intercept data packets. It can be legitimate (for troubleshooting) or malicious (for eavesdropping or data theft).

Packet Spoofing: In packet spoofing, an attacker falsifies packet headers (e.g., source IP address) to deceive systems or networks. It can lead to unauthorized access or denial-of-service attacks.

Denial of Service (DoS): A DoS attack floods a system or network with excessive traffic, rendering it unavailable to legitimate users. The goal is to disrupt services or cause downtime.

Forged Routing: Forged routing involves manipulating routing tables or protocols to redirect network traffic. Attackers can reroute data to unauthorized destinations.

Port Scanning: Port scanning identifies open ports on a system or network. While legitimate for network administrators, malicious port scanning can reveal vulnerabilities for exploitation.

Security Scanning: Security scanning assesses systems for vulnerabilities, misconfigurations, or weaknesses. Regular scans help maintain security and prevent unauthorized access.

Browser Extension: A browser extension is a small software module that enhances a web browser's functionality. Users install extensions to customize their browsing experience.

Junk Mail: Junk mail (also known as spam) refers to unsolicited and often irrelevant emails sent in bulk. It clutters inboxes and may contain phishing attempts or malware.

Hosted Service: Refers to a service provided by a third party that hosts and manages software applications, infrastructure, or platforms on behalf of clients. These services are typically accessed over the internet and can include:

Software as a Service (SaaS): Applications hosted and managed by a third party, accessible via a web browser (e.g., email services, CRM systems).

Platform as a Service (PaaS): Platforms for developing, testing, and deploying applications, managed by a third party (e.g., cloud-based development environments).

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

Infrastructure as a Service (IaaS): Virtualized computing resources such as servers, storage, and networking, provided and managed by a third party (e.g., cloud storage services).

V. Policy Terms & Provisions

A. General Use and Ownership

1. Users should be aware that the data they create on City Systems remains the property of the City of Bend and will generally be considered and treated as public records subject to the retention and disclosure requirements of state law.

2. Users should exercise good judgment regarding the reasonableness of personal use including time spent, timing of personal use, and content accessed or created. An employee's access to City-issued devices is not intended to replace need for personal devices. If there is any uncertainty, users should consult the employee handbook, as applicable, their supervisor, and/or the IT Department.

3. All data is handled with sensitivity and care. Data encryption can be used as an additional protection layer for storing and transmitting data; encryption must be used for all data the City determines is sensitive.

4. The City may monitor and/or audit City Systems, and any network traffic, content, and any other information or data at any time.

B. Security and Proprietary Information

1. Users are required to complete the required cybersecurity training coordinated by the IT Department to ensure they are aware of security policies, practices, and user responsibilities while using City Systems.

2. Users must report suspicious activity immediately to the IT Department or the Information Security Manager.

3. Users should take all necessary steps to prevent unauthorized access to City Systems and any related information and data.

4. If a City device assigned to a user is damaged, lost, or stolen, the user should report the incident to the IT Service Desk immediately.

5. Users must keep passwords secure and not share account login or access information or credentials with any other party, unless directed to do so by authorized City staff for purposes such as technical support or other legitimate business purpose. Passwords shall adhere to the City of Bend **Password Policy**.

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

6. All hardware, including but not necessarily limited to PCs, laptops, workstations, and servers, should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Windows users) when the device will be unattended. In extenuating circumstances these policies may be adjusted with the approval and assistance of the IT Department.

7. External access to City Systems by vendors, contractors, or third-party contributors must be done using City of Bend technology and procedures approved by the City IT Department.

8. Artificial Intelligence (AI) use must comply with City and Information Technology policies.

9. Caution must be exercised when accessing City of Bend technology systems.

C. Unacceptable Use

Under no circumstances is any user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City Systems.

The sections below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

D. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. The installation of software, hardware, or the purchase of a hosted service that is not approved by the IT Department.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Bend does not have an active license is strictly prohibited.

3. Significant consumption of City Systems resources for non-business-related activities (such as video, audio or downloading large files) or excessive time spent using City Systems or access for non-business purposes (e.g., shopping, social networking, sports related sites). The City reserves the right to determine whether consumption is significant and in violation of this Policy by evaluating, among other factors, whether the consumption is creating impacts to City Systems and the ability of the City or its employees to carry out their work effectively and efficiently.

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

4. Introduction of malicious programs into City Systems (e.g., viruses, worms, Trojan horses, malware, etc.) Although this can happen inadvertently, users of City Systems maintain responsibility for understanding and employing best practices to maintain security and integrity of City Systems.

5. Revealing an account password to others or allowing use of a user's account by others. This includes co-workers, family, and other household members.

6. Allowing access to City Systems by unauthorized parties, including co-workers, vendors, family, and other household members.

7. Using City Systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or laws related to workplace conduct or behavior.

8. Making fraudulent offers of products, items, or services originating from City Systems.

9. Effecting the security of City Systems including security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless this activity is a part of the user's normal job/duty.

11. Executing any form of network monitoring which will intercept data unless this activity is a part of the user's normal job/duty.

12. Circumventing user authentication or security of any system or account.

13. Interfering with or denying service to any system or account (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, the normal operations of a system.

15. Accessing content that is prohibited by the City, including but not necessarily limited to the Network Filtering and Browser Extension Policy in the Policy Hub.

16. Connecting computers or systems that are not authorized by the IT Department to City Systems is prohibited.

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

E. Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment using City Systems, whether through language, frequency, size of messages, or other means.

3. Any form of impersonation.

4. Unsubscribing, blocking, filtering, or rerouting City of Bend official communications.

5. Any personal commercial purpose that is not City business.

6. Any purpose involving a political campaign.

7. The transmission of confidential or sensitive information to unauthorized recipients.

8. Providing information about, or lists of, the City of Bend employees to parties outside the City of Bend, outside of the normal public disclosure process.

F. Social Media Activities

1. Limited and occasional use of City Systems to engage in social media is acceptable, if it is done in a professional and responsible manner, does not otherwise violate the City of Bend's Employee Handbook, this policy or other City policies, is not detrimental to the City of Bend's best interests, and does not interfere with any work duties. Social media activity from City Systems is also subject to auditing, monitoring and all other applicable elements of this Policy.

2. The City of Bend's Confidential Information policy under section 2.3 of the Employee Handbook also applies to social media. As such, users are prohibited from revealing any City of Bend confidential or proprietary information when engaged in social media activity. Users shall not engage in any social media posting that may harm or tarnish the image, reputation and/or goodwill of the City of Bend and/or any of its employees. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when social media posting or otherwise engaging in any conduct prohibited by the City of Bend's Non-Discrimination and Anti-Harassment policy under section 5.6 of the Employee Handbook.

3. Users may not attribute personal statements, opinions or beliefs to the City of Bend when engaged in social media activity. If a user is expressing their beliefs and/or

Docusign Envelope ID: 3733E123-E8B4-4BCC-900B-65A66FA67B5F

opinions on social media using City Systems, the user may not, expressly, or implicitly, represent themselves as an employee or representative of the City of Bend. Users assume any and all risk associated with personal social media activity using City Systems.

4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the City of Bend's trademarks, logos, and any other City of Bend intellectual property may not be used in connection with any social media activity unless authorized by the City of Bend Communications Department.

Language Assistance Services & Accommodation Information for People with Disabilities
You can obtain this information in alternate formats such as Braille, electronic format, etc. Free language assistance services are also available. Please contact Juan Olmeda at **jolmeda@bendoregon.gov** or 541-388-5505. Relay Users Dial 7-1-1.

Servicios de asistencia lingüística e información sobre alojamiento para personas con discapacidad
Puede obtener esta información en formatos alternativos como Braille, formato electrónico, etc. También disponemos de servicios gratuitos de asistencia lingüística. Póngase en contacto con Juan Olmeda en **jolmeda@bendoregon.gov** o 541-388-5505. Los usuarios del servicio de retransmisión deben marcar el 7-1-1.

Certificate Of Completion

Envelope Id: 3733E123-E8B4-4BCC-900B-65A66FA67B5F
Status: Completed
Subject: Complete with Docusign: IT-0001 IT Acceptable Use Policy.pdf
Source Envelope:
Document Pages: 8
Signatures: 2
Certificate Pages: 5
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Envelope Originator:
Brenda Mingus
710 NW Wall St.
Bend, OR 97703
bmingus@bendoregon.gov
IP Address: 10.103.81.73

Record Tracking

Status: Original
4/30/2025 3:11:43 PM
Holder: Brenda Mingus
bmingus@bendoregon.gov
Location: DocuSign

Signer Events	Signature	Timestamp
Ian M. Leitheiser ileitheiser@bendoregon.gov Asisstant City Attorney Security Level: Email, Account Authentication (None)	Signed by: Ian M. Leitheiser 392FD2178C27458... Signature Adoption: Pre-selected Style Using IP Address: 98.142.36.35	Sent: 4/30/2025 3:12:18 PM Viewed: 4/30/2025 3:13:20 PM Signed: 4/30/2025 3:13:36 PM
Electronic Record and Signature Disclosure: Accepted: 4/30/2025 3:13:20 PM ID: 8cd011ea-eb0e-4339-8e0c-8890dd2f3ee4 Company Name: City of Bend		
Eric King eking@bendoregon.gov City Manager City of Bend Security Level: Email, Account Authentication (None)	DocuSigned by: Eric King 409FF33EB4E64D3... Signature Adoption: Pre-selected Style Using IP Address: 174.204.194.238 Signed using mobile	Sent: 4/30/2025 3:13:37 PM Viewed: 4/30/2025 3:16:24 PM Signed: 4/30/2025 3:16:33 PM
Electronic Record and Signature Disclosure: Accepted: 5/11/2021 3:40:52 PM ID: 1be4d586-76d4-4e39-83e4-3feae319b4d0 Company Name: City of Bend		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	4/30/2025 3:12:18 PM
Certified Delivered	Security Checked	4/30/2025 3:16:24 PM
Signing Complete	Security Checked	4/30/2025 3:16:33 PM
Completed	Security Checked	4/30/2025 3:16:33 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, City of Bend (we, us or City) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you may be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below. Paper copies may also be requested from City by contacting Procurement.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

Notices and disclosures may be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we may provide electronically to you through the DocuSign system required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. You can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact the City:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To advise the City of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at dgalanaugh@bendoregon.gov and in the body of such request you must state: your previous email address, your new email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to dgalanaugh@bendoregon.gov and in the body of such request you must state your email address, full name, mailing address, and telephone number.

To withdraw your consent with the City

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to dgalanaugh@bendoregon.gov and in the body of such request you must state your email, full name, mailing address, and telephone number.

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- **You can access and read this Electronic Record and Signature Disclosure; and**
- **You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and**
- **Until or unless you notify the City as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by the City during the course of your relationship with the City.**